IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellants:	Mendonca, J.	Patent Application	
Application Number:	10/627,017	Group Art Unit:	2136
Filed:	July 25, 2003	Examiner:	Okoronkwo, C.

For: METHOD OF MANAGING UTILIZATION OF NETWORK INTRUSION DETECTION SYSTEMS IN A DYNAMIC DATA CENTER

APPEAL BRIEF

Table of Contents

I. Real Party in Interest

The assignee of the present invention is Hewlett-Packard Development Company, L.P.

II. Related Appeals and Interferences

There are no related appeals or interferences known to the Appellants.

III. Status of Claims

Claims 1- 20 are rejected. This Appeal involves Claims 1-20.

IV. Status of Amendments

All proposed amendments have been entered. An amendment subsequent to the Final Action has not been filed.

V. Summary of Claimed Subject Matter

Independent Claims 1, 8, and 15 of the present application pertain to embodiments associated with methods and systems for managing utilization of network intrusion detection systems in a dynamic data center.

As recited in Claim 1, a "method of managing utilization of network intrusion detection systems in a dynamic data center" is disclosed. One embodiment is depicted at least in Figures 1 and 2. As described in the instant disclosure on page 7, lines 20-30, Figure 1 and 210 of Figure 2, one method includes providing a plurality of network intrusion detection systems 70, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center 100. The instant disclosure further includes on page 8, lines 1-6, and 220 of Figure 2, receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems 70. Furthermore, the instant disclosure includes on page 8, lines 8-10 and 230 of Figure 2, automatically arranging the monitoring of said monitoring points using said network intrusion detection systems 70 and said monitoring policy.

As recited in Claim 8, a "method of managing utilization of network intrusion detection systems in a dynamic data center" wherein "a computer-readable medium comprising computer-executable instructions stored therein" for performing the method is disclosed. One embodiment is depicted at least in Figures 1 and 2. As described in the instant disclosure on page 7, lines 20-30, Figure 1 and 210 of Figure 2, one method includes providing a plurality of network intrusion detection systems 70, each being networked so that utilization of each network intrusion detection system can be based on demand for said

network intrusion detection systems in said dynamic data center 100. The instant disclosure further includes on page 8, lines 1-6, and 220 of Figure 2, receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems 70. Furthermore, the instant disclosure includes on page 8, lines 8-10 and 230 of Figure 2, automatically arranging the monitoring of said monitoring points using said network intrusion detection systems 70 and said monitoring policy.

As recited in Claim 15, a system comprising "a dynamic data center" 100 is disclosed. One embodiment is depicted at least in Figure 1. As described in the instant disclosure on at least page 5, lines 23-24 and Figure 1, one embodiment includes a dynamic data center 100 including a plurality of network resources 60. On at least page 7, lines 27-30 and Figure 1, the instant disclosure includes a plurality of network intrusion detection systems 70, each being networked so that utilization of each network intrusion detection system 70 can be based on demand for the network intrusion detection systems 70 in the dynamic data center 100. Furthermore, the instant disclosure includes at least on page 7, lines 5-18 and Figure 1, a graphical user interface 20 for receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of the network intrusion detection systems 70. Moreover, the instant disclosure includes at least on page 8, lines 8-10 and Figure 1, a controller 10 for controlling the network resources 60 and the network intrusion detection systems 70 and for automatically arranging the monitoring of the monitoring points using the network intrusion detection systems 70 and the monitoring policy.

VI. Grounds of Rejection to Be Reviewed on Appeal

1. Claims 1-20 are rejected under 35 U.S.C. §102(e) as being anticipated by Shanklin, et al. (U.S. Patent No. 6,578,147) (hereinafter, "Shanklin").

VII. Argument

1. Whether Claims 1-20 are anticipated by Shanklin.

Appellants respectfully submit that embodiments of the present invention as recited in Claims 1-20 are not anticipated by Shanklin, in view of the following rationale.

Appellants respectfully point out that independent Claim 1 (Claims 8 and 15 include similar features) recites a method of managing utilization of network intrusion detection systems in a dynamic data center, said method comprising:

> providing a plurality of network intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center;
>
> receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems; and
>
> automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy.

(Emphasis added.)

Appellants respectfully note that "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference". MPEP §2131; *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 103 (Fed. Cir. 1987).

The instant Office Action states the following:

> [r]egarding the second limitation ["receiving a monitoring policy…], the Examiner directs the Applicant to column 2 lines 1-13 in which Shanklin et al. discloses the claimed "monitoring policy" as being inclusive to the IDS sensors, which comprise:

> "packet load to the sensors that is 'load balanced', such that said packets are distributed at least at a session-based level [or] packet-based level … the results of the detection performed by the sensors and the network analyzer are used to determine if there is an attempt to gain unauthorized access to the network.

(Emphasis in original; Office Action mailed on August 5, 2008 [hereinafter, "instant Office Action"]) The instant Office Action seems to be equating Shanklin's session-based and packet-based load balancing with "receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems" as is recited in Appellants' Claim 1.

Shanklin further describes "session-based" and "packet-based" load balancing. For example, Shanklin describes session-based load balancing as the following:

> that each sensor 21 handles a portion of the sessions incoming to the network. A stream of packets, S1, S2, … S6, … is illustrated. In the example of FIG. 2, the load balancing is such that S1 goes to a first sensor, S2 to a second, S3 to a third, S4 to the first, and so on. Thus, each sensor 21 handles one-third of the sessions in a given datastream.

(Emphasis added; Shanklin, Column 5, lines 21-29.) Shanklin describes packet-based load balancing to mean the following:

> Router 32 has a load balancing unit 32a, which distributes a packet stream comprised of packets P1, P2, … P6 …. The load balancing is such that P1 goes to a first sensor, P2 to a second, P3 to a third, P4 to the first, and so on.

(Shanklin, column 5, lines 56-62.)

Appellants understand Shanklin to disclose a session-based load balancing in which a session of a series of sessions are distributed to each sensor of multiple sensors, and a packet-

based load balancing in which packets are distributed to each sensor of multiple sensors. Shanklin focuses on distributing sessions and packets to and among all sensors that detect "signatures of attacks" (Shanklin, column 5, line 37). However, Shanklin remains silent as to a dynamic system that receives "a monitoring policy and a plurality of monitoring points to be monitored" (emphasis added) as is recited in Appellants' Claim 1.

Therefore, Appellants respectfully submit that Shanklin does not anticipate the Appellants' invention as is set forth in independent Claims 1, and as such, Claim 1 traverses the Examiner's basis for rejection under 35 U.S.C. §102(e) and is in condition for allowance. Accordingly, Appellants also respectfully submit for similar reasons that Shanklin does not anticipate the present claimed invention as is recited in Claims 8 and 15. Furthermore, Appellants respectfully submit that Claims 2-7 depending on Claim 1, Claims 9-14 depending on Claim 8, and Claims 16-20 depending on Claim 15 overcome the rejection under 35 U.S.C. §102(e) as being dependent on an allowable base claim.

CONCLUSION

Appellants believe that pending Claims 1-20 are directed toward patentable subject matter. As such, Appellants respectfully request that the rejections of Claims 1-20 be reversed.

The Appellants wish to encourage the Examiner or a member of the Board of Patent Appeals to telephone the Appellants' undersigned representative if it is felt that a telephone conference could expedite prosecution

Respectfully submitted,
WAGNER BLECHER LLP

Dated: 11/17/2008

/John P. Wagner, Jr./
John P. Wagner, Jr.

Registration No. 35,398

Wagner Blecher LLP
123 Westridge Drive
Watsonville, CA 95076
(408) 377-0500

VIII. Appendix - Clean Copy of Claims on Appeal

1. A method of managing utilization of network intrusion detection systems in a dynamic data center, said method comprising:

providing a plurality of network intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center;

receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems; and

automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy.

2. The method as recited in Claim 1 wherein said automatically arranging the monitoring of said monitoring points includes:

automatically configuring a plurality of network resources to provide network communication data from said monitoring points to a plurality of available network intrusion detection systems from said network intrusion detection systems; and

automatically configuring said available network intrusion detection systems to receive said network communication data based on said monitoring policy.

3. The method as recited in Claim 2 wherein said automatically arranging the monitoring of said monitoring points further includes:

automatically increasing a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by selecting additional available network intrusion detection systems if said network communication data exceeds a capacity of said particular network intrusion detection systems.

4. The method as recited in Claim 2 wherein said automatically arranging the monitoring of said monitoring points further includes:

automatically decreasing a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by releasing any of said particular network intrusion detection systems to said available network intrusion

detection systems if said network communication data is below a predetermined threshold of a capacity of said particular network intrusion detection systems.

5. The method as recited in Claim 2 wherein said network resources include one of a firewall, a gateway system, a network switch, and a network router.

6. The method as recited in Claim 1 wherein said receiving a monitoring policy and a plurality of monitoring points to be monitored includes:

providing a graphical user interface to receive said monitoring policy and said plurality of monitoring points to be monitored.

7. The method as recited in Claim 1 wherein said dynamic data center is a utility data center.

8. A computer-readable medium comprising computer-executable instructions stored therein for performing a method of managing utilization of network intrusion detection systems in a dynamic data center, said method comprising:

providing a plurality of network intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center;

receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems; and

automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy.

9. The computer-readable medium as recited in Claim 8 wherein said automatically arranging the monitoring of said monitoring points includes:

automatically configuring a plurality of network resources to provide network communication data from said monitoring points to a plurality of available network intrusion detection systems from said network intrusion detection systems; and

automatically configuring said available network intrusion detection systems to receive said network communication data based on said monitoring policy.

10. The computer-readable medium as recited in Claim 9 wherein said automatically arranging the monitoring of said monitoring points further includes:

automatically increasing a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by selecting additional available network intrusion detection systems if said network communication data exceeds a capacity of said particular network intrusion detection systems.

11. The computer-readable medium as recited in Claim 9 wherein said automatically arranging the monitoring of said monitoring points further includes:

automatically decreasing a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by releasing any of said particular network intrusion detection systems to said available network intrusion detection systems if said network communication data is below a predetermined threshold of a capacity of said particular network intrusion detection systems.

12. The computer-readable medium as recited in Claim 9 wherein said network resources include one of a firewall, a gateway system, a network switch, and a network router.

13. The computer-readable medium as recited in Claim 8 wherein said receiving a monitoring policy and a plurality of monitoring points to be monitored includes:

providing a graphical user interface to receive said monitoring policy and said plurality of monitoring points to be monitored.

14. The computer-readable medium as recited in Claim 8 wherein said dynamic data center is a utility data center.

15. A system comprising:

a dynamic data center including:

a plurality of network resources;

a plurality of network intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center;

a graphical user interface for receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems; and

a controller for controlling said network resources and said network intrusion detection systems and for automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy.

16. The system as recited in Claim 15 wherein said controller automatically configures said network resources to provide network communication data from said monitoring points to a plurality of available network intrusion detection systems from said network intrusion detection systems, and wherein said controller automatically configures said available network intrusion detection systems to receive said network communication data based on said monitoring policy.

17. The system as recited in Claim 16 wherein said controller automatically increases a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by selecting additional available network intrusion detection systems if said network communication data exceeds a capacity of said particular network intrusion detection systems.

18. The system as recited in Claim 16 wherein said controller automatically decreases a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by releasing any of said particular network intrusion detection systems to said available network intrusion detection systems if said network communication data is below a predetermined threshold of a capacity of said particular network intrusion detection systems.

19. The system as recited in Claim 15 wherein said network resources include one of a firewall, a gateway system, a network switch, and a network router.

20. The system as recited in Claim 15 wherein said dynamic data center is a utility data center.

IX. Evidence Appendix

No evidence is herein appended.

X. Related Proceedings Appendix

No related proceedings.